

Lawrence Berkeley National Laboratory

GPO Policies and Procedures

GPO Guidelines

Planning

- Establish consensus as appropriate to your unit
- Consider ramifications of each policy applied
- Communicate your GPO plan to affected users
- Follow the LBLAD guidelines for managing GPO's

Creation

- Follow LBL Active Directory standard naming conventions. The LBL recommended naming standard for Active Directory Group Policy Objects (GPOs) is: OUName-GPOName, where OUName is your OU name and GPOName is a descriptive name that explains the purpose of the GPO. ***This naming standard is important because it is the primary mechanism to prevent OU Managers from accidentally linking another admin's GPO to their OU.***
- The Linking policies feature is not supported in the LBL Active Directory. This feature can lead to increased time troubleshooting GPO's, adds unnecessary complexity to the implementation of GPO's, and may disrupt the users' environment.
- OU Admins should document their GPO's in the manner described above
- The use of "Blocking Policy Inheritance" is not supported in the LBL Active Directory. Applying a Policy Inheritance Block may interfere with approved domain policies.
- The use of "Deny ACE's" while filtering GPO's is not supported in the LBL Active Directory. Denying ACE's could; lead to increased time spent troubleshooting GPO's, add unnecessary complexity to the implementation of GPO's, and/or disrupt the users' environment. OU Admins can use group filtering as an alternative to using a "Deny ACE"
- OU Admins should contact interested/affected users in a timely manner when policies are created/newly applied to users.

How Group Policies are Applied

- Inherited and cumulative and will affect all computers in an OU if not filtered.
- Processed in the following order: local (workstation), site, domain, and OU
- As each policy is processed, its settings are merged into the registry
- If multiple policies are applied to a computer, the effective policy is the result of merging, in order, all policies defined for the computer

LBLAD Policies on GPOs

- OU Admins are the only authorized parties to change/delete GPO's in their Organizational Unit
- OU Admins should contact interested/affected users in a timely manner when policies are being changed or deleted
- Changed/Deleted GPO's must be documented in the published share.
- Documentation for deleted GPO's should remain in the documentation folder for 1 year.